State of Indiana Policy and Standards

Authorized Software

Standard ID
IOT-CS-SEC-001

Published Date
9/1/2016

Effective Date
1/2/2017

Last Updated
9/27/2016

Next Review Date
9/27/2017

Policy
09.0 Information Protection Processes and Procedures (PR.IP)

09.1 PR.IP-1

09.1.1 Configuration Management

Purpose
Unauthorized software can introduce unmanaged, vulnerable software into the State environment, which can be used by attackers to exploit hosts and further compromise them. There can also be legal issues with the installation of unauthorized software, such as violations of licensing agreements. This standard provides the requirements for installing and maintaining software, fulfilling a well-controlled desktop environment.

Scope
IOT Supported Entities

Statement
A standard baseline workstation/laptop or virtual image will include applications/software that is provided and maintained by IOT. Installation of additional software located in IOT's maintained list (e.g., software center) or on IOT's published 'Whitelist' applications are permissible for installation without additional forms, provided that the software licenses, security updates, patches and other maintenance is kept up to date by the agency(s) using it.

All additional software requests that do not meet the criteria above shall be formally reviewed by the agency's information security resources and IOT. A completed Software Authorization Request Form must be sent to the IOT Security distribution list for review. Provided that there is approval, the agency is responsible and agrees to maintain all components of the software, including (but no limited to):

- Maintaining compliance with software license requirements
- Notifying IOT and indicating the latest security updates and patching that need to be installed
- Performing appropriate tests to confirm proper installation and functionality

Software that has been illegally copied, downloaded from an unauthorized source or is unauthorized shareware/freeware is not authorized for use on the State network.

Installation of software on State resources by unauthorized personnel is prohibited.

If any unauthorized software is found on State devices, software shall be removed by IOT and escalations will be sent to Agency Heads and the CISO.

Roles

All Personnel

Responsibilities

All personnel shall go through the appropriate process for additional software requests. Anyone aware of unauthorized software shall report this to the Director of Risk & Compliance or the CISO.

Management Commitment

Management shall ensure that all software is authorized for their respective agency.

Coordination Among Organizational Entities

Agencies shall coordinate with IOT for adding additional software to devices and maintain additional software only for business purposes.

Compliance

Management can request reporting from IOT for installed software on their agency machines. All unauthorized software shall be removed.

Exceptions

Exceptions will be handled on a case by case basis through the Director of Risk & Compliance and State CISO.

Associated Links

Software Authorization Request Form